CVE Board Meeting Notes
April 27, 2022 (2:00 pm – 4:00 pm ET)

CVE Board Attendance

☐Ken Armstrong, EWA-Canada, An Intertek Company
☒Tod Beardsley, Rapid7
☐Chris Coffin (MITRE At-Large), The MITRE Corporation
☐Jessica Colvin
☒Mark Cox, Red Hat, Inc.
☐William Cox, Synopsys, Inc.
☒Patrick Emsweller, Cisco Systems, Inc.
☐Jay Gazlay, Cybersecurity and Infrastructure Security Agency (CISA)
☐Tim Keanini, Cisco Systems, Inc.
☒Kent Landfield, Trellix
☒Scott Lawler, LP3
☐Chris Levendis (MITRE, Board Moderator), CVE Program
☐Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
☐Pascal Meunier, CERIAS/Purdue University
☐Tom Millar, Cybersecurity and Infrastructure Security Agency (CISA)
☐Ken Munro, Pen Test Partners LLP
☒Chandan Nandakumaraiah, Palo Alto Networks
☒Kathleen Noble, Intel Corporation
☒Lisa Olson, Microsoft
☒Shannon Sabens, CrowdStrike
☒Takayuki Uchiyama, Panasonic Corporation
☒David Waltermire, National Institute of Standards and Technology (NIST)
☒James “Ken” Williams, Broadcom Inc.

MITRE CVE Team Attendance

☒ Kris Britton
☒ Christine Deal
☒ Dave Morse
☒ Art Rich

Agenda

- 2:00-2:05 Introduction
- 2:05-3:35 Agenda and Open Discussion
  - Cloudy with Chance of CVE
  - Working Group Updates
  - Overview of Outstanding Documents
  - Unmaintained Open-Source Software
  - Open Discussion
- 3:35-3:55 Review of Action Items
- 3:55-4:00 Next Meetings and Future Agenda Topics

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
04.27.01	Look into blog post examples that may be helpful to guide our messaging about cloud vulnerabilities.	Lisa Olson	
04.27.02	Contact the journalist who wrote the article "Firms Push for CVE-Like Cloud Bug System," and request that, for future articles about CVE, please contact the CVE Program first to ensure accuracy.	Tod Beardsley	
04.27.03	Draft a blog writeup about the Program's position and process for cloud vulnerabilities. This will be for Board review.	Chris Levendis	
04.27.04	Reach out to the responsible CNA for CVE ID (CVE-2022-24409) and explain what they need to do to improve the description (does not include public disclosure and information about the nature of the vulnerability). Treat it as an opportunity to teach the CNA.	Secretariat	

Cloudy with Chance of CVE (Tod Beardsley)

- Discussion was in the context of an article at ThreatPost called "Firms Push for CVE-Like Cloud Bug System" located here.
- The Board decided a few years ago that if a cloud provider finds an issue that warrants a CVE ID, the provider CNA can assign an ID for that issue, but it is at the discretion of the provider.
- There is a perception that the CVE Program does not deal with cloud vulnerabilities, which is not true.
- Better messaging to the community is needed, e.g., blog, podcast, to get the point across that the program does work with cloud issues, and the associated process.

- **Action**: Lisa O. may have blog post examples. She will look into this and report back to the Board.
- **Action**: Tod B. will contact the journalist who wrote the article and request that, for future articles about CVE, contact the CVE Program first to help ensure accuracy.
- **Action**: Chris L. will draft a blog writeup for Board review.

Working Group Updates

- Automation Working Group (AWG) (Kris Britton)
  - AWG is working through the 23 findings identified in penetration testing that ended mid-March. These findings need to be addressed prior to CVE Services deployment.
  - The findings are being fixed using multiple two-week remediation sprints. Currently, the team is in the middle of sprint 3 of a predicted 5 sprint effort.
  - AWG is meeting weekly with the Transition Working Group (TWG) to keep them up to date on progress/status.
  - Community members are contributing to the remediation effort, specifically Octopus Deploy, who has been contributing to the code base.
  - A significant finding was related to the 22 CVE Services application programming interfaces (API) and how they were not very well defined and documented. The AWG has a consensus that Swagger technology should be used to automatically generate API specifications. Alot of work is going into remediating the API finding.
  - A new deployment date will not be announced until there is high confidence that the program has functioning CVE Services with the 22 APIs.
  - The AWG has also been working on: a client engagement strategy for CVE Services; developing criteria (also called scorecard) to determine deployment readiness (expected to be done in the next two weeks); and working with the community to think about the threat environment.
  - Once AWG (using the criteria for deployment) makes the recommendation to deploy, reviews will be done by SPWG, and then the Board for decision. The Secretariat will also have to agree before deployment happens.
- Quality Working Group (QWG) (Dave Waltermire)
  - Tracking issues that come up in AWG's work.
  - Continuing to work with CNAs to correct some of their record details.
  - Making updates to the conversion scripts to fix a few small issues that have been identified.
  - Waiting until JSON 5 record format is deployed before starting on a 5.1 release of the format.
- CNA Coordination Working Group (CNACWG) (Tod Beardsley)
  - Launched a CNA mentoring program a week ago, and there have been 16 responses, more than expected. Of those, only one is not yet matched up with a mentor.

Responses included CNAs that want to be mentored and CNAs who want to provide mentoring support.

  - The WG owes Shannon S. a draft of the talk that Tod is giving at RSA in June. The talk will be 20 minutes and will focus on the CVE Program, what Rapid7 is doing in that space, and why people or organizations should become CNAs. The target is to have a draft written by the next Board meeting.

- Strategic Planning Working Group (SPWG) (Kent Landfield)
  - SPWG is taking a hiatus for the next few months (estimate: until mid-July). Future work (e.g., the two ADP pilots) is dependent on deployment of CVE Services.
  - In the meantime, use the mailing list for matters that involve SPWG. Also, ad-hoc meetings can be held as needed.
- Transition Working Group (TWG) (Lisa Olson)
  - There are different types of CNAs. A small CNA (for example, 1-2 IDs/records per year) can continue to use the web form on the CVE Program website. CVE Services is not really geared toward their needs. A medium CNA (for example, they create 10 to 15 IDs at a time) wants a more streamlined approach, and it is not a big burden to use JSON 5 with Vulnogram to create the data structure, and then output it to a file and submit through the Red Hat client in a bulk way. Large CNAs will probably want to use the API.

Overview of Outstanding Documents (Dave Morse)

- The status of three in-work program documents was shared with the Board.
- The *CVE Governance and Organization* document is a new document. It uses material from Program Rules v3, and it updates organizational names that have changed. For example, there are no longer Root-CNAs and Sub-CNAs, just CNAs, CNAs-LR, Roots, and TL-Roots. More review is needed, but it is significantly complete from a content perspective.
- The *CNA Operational Rules* document is undergoing an update to v3 to focus on rules (not organizational structure), update organizational names, and make recommended updates from v3 SPWG review. Further progress is waiting for CVE Services deployment.
- The *CVE Working Group Operations Handbook* is undergoing an update to v2. It is close to completion, needing just a final review by the Secretariat before submission to the Board for review/approval.

Unmaintained Open-Source Software

- Consensus was that “no longer maintained” does not equal a vulnerability. Users of unmaintained software take on a risk, but that is not necessarily a CVE vulnerability. If a vulnerability has been identified, it can be assigned a CVE ID.

Open Discussion

- Dave W. identified a CVE ID (CVE-2022-24409) that includes language in its description about no public disclosure until a later date. That is an inadequate description since the CVE

Program is about public disclosure. The description also does not provide information about the nature of the vulnerability, so it is inadequate in that respect.

  - **Action**: Secretariat (CNA Coordination Team) to reach out to the responsible CNA and explain what they need to do to improve the description. Treat it as an opportunity to teach the CNA.

- For anyone planning to attend RSA, let others know so there is an opportunity for some face-to-face time with colleagues.

Review of Open Action Items

- Action item 10.28.01 (Working Group Operations Handbook). Add comment to the action item log that one final review is needed by the Secretariat prior to submission to the Board for review/approval.
- Action item 09.30.04 (CVE Dispute Policy). Add comment to the action item log that the policy has been drafted and is expected to be distributed for internal Secretariat review in the next day or two. This review will be followed by Council of Roots review, and finally Board review. The policy will include how to address dispute tagging: The tag will go either into the CNA or ADP container, depending on who is making the dispute.

Next CVE Board Meetings

- Wednesday, May 11, 2022, 9:00am – 11:00am (ET)
- Wednesday, May 25, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, June 8, 2022, 9:00am – 11:00am (ET)
- Wednesday, June 22, 2022, 2:00pm – 4:00pm (ET)

Discussion Topics for Future Meetings

- CVE Services updates, as needed
- Summit planning updates
- CVE Program website transition progress, as needed
- Council of Roots meeting highlights
- Working Group updates, every other meeting
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report